UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/748,996	12/27/2000	Douglas B. Quine	F-184	6428

919 7590 10/01/2004

PITNEY BOWES INC.
35 WATERVIEW DRIVE
P.O. BOX 3000
MSC 26-22
SHELTON, CT 06484-8000

EXAMINER	
POKRZYWA, JOSEPH R	

ART UNIT	PAPER NUMBER
2622	

DATE MAILED: 10/01/2004 5

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/748,996	**Applicant(s)** QUINE, DOUGLAS B.
	Examiner Joseph R. Pokrzywa	**Art Unit** 2622

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)□ Responsive to communication(s) filed on _____.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 December 2000* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Drawings

1. The drawings received on 12/27/00 are acceptable by the examiner.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. **Claims 1 and 11** are rejected under 35 U.S.C. 102(b) as being anticipated by Grundy (U.S. Patent Number 5,291,598).

Regarding ***claim 1***, Grundy discloses a system for authenticating information communicated over a network (see Fig. 1, column 6, line 55-column 7, line 21), comprising an originating device (see Fig. 1, column 6, line 51-column 7, line 35), the originating device comprising means for generating data representative of data received by the originating device (column 15, lines 28-68, column 18, line 34-column 19, line 18, and column 21, lines 29-60), means for computing a checksum of the input data (column 15, lines 28-68, column 18, line 34-column 19, line 18, and column 21, lines 29-60), means for encrypting the computed checksum, thereby generating an encrypted checksum data (column 15, lines 28-68, column 18, line 34-

column 19, line 18, and column 21, lines 29-60), means for convolving the representative data and the encrypted checksum data thereby producing a convolved data (column 15, lines 28-68, column 18, line 34-column 19, line 18, and column 21, lines 29-60), means for communicating the convolved data to a destination device (column 15, lines 28-68, column 18, line 34-column 19, line 18, and column 21, lines 29-60), the destination device comprising means for computing checksum of data received at the destination device (column 15, lines 3-40, column 18, line 45-column 19, line 18), means for decrypting the encrypted checksum data from convolved data (column 15, lines 46-68, and column 18, line 45-column 20, line 34), means for comparing the decrypted checksum data with checksum computed by the destination device in order to verify the authenticity of information received by the destination device (column 15, lines 46-68, and column 18, line 45-column 20, line 34), and means for alerting a recipient at the destination device in the event of a mismatch between the decrypted checksum data and the checksum computed by the destination device (column 14, line 64-column 15, line 45, see Fig. 3).

Regarding ***claim 11***, Grundy discloses a system for authenticating information transmitted via a communications network (see Fig. 1, column 6, line 55-column 7, line 21), comprising a transmitting apparatus for converting an original input data into a first format (see Fig. 1, column 6, line 51-column 7, line 35), the transmitting apparatus further comprising means for computing an encrypted checksum representing the input data (column 15, lines 28-68, column 18, line 34-column 19, line 18, and column 21, lines 29-60), a receiving apparatus for receiving data in the first format from the transmitting apparatus (see Fig. 1, column 6, line 51-column 7, line 35), the receiving apparatus further comprising means for computing checksum of the received data (column 15, lines 3-40, column 18, line 45-column 19, line 18), a decrypting means for decrypting the encrypted checksum (column 15, lines 46-68, and column 18, line 45-column 20, line 34), and means for comparing the decrypted checksum with checksum of the received data, and alerting a recipient at the receiving apparatus in the event of a mismatch (column 14, line 64-column 15, line 45, see Fig. 3).

4. **Claims 1 and 11** are rejected under 35 U.S.C. 102(e) as being anticipated by Klein (U.S. Patent Number 6,259,367).

Regarding ***claim 1***, Klein discloses a system for authenticating information communicated over a network (see Figs. 1-8), comprising an originating device (see Fig. 1), the originating device comprising means for generating data representative of data received by the originating device (see Figs. 6 and 7), means for computing a checksum of the input data (steps 218-220), means for encrypting the computed checksum, thereby generating an encrypted checksum data (steps 218-222), means for convolving the representative data and the encrypted checksum data thereby producing a convolved data (step 222-226), means for communicating the convolved data to a destination device, the destination device (column 9, line 52-column 10, line 21) comprising means for computing checksum of data received at the destination device (steps 218-222, column 10, lines 7-21), means for decrypting the encrypted checksum data from convolved data (steps 220-222, column 10, lines 7-21), means for comparing the decrypted checksum data with checksum computed by the destination device in order to verify the authenticity of information received by the destination device (see Fig. 8, steps 224-228, column 10, lines 7-21), and means for alerting a recipient at the destination device in the event of a mismatch between the decrypted checksum data and the checksum computed by the destination device (see Fig. 8, steps 224-228, column 10, lines 7-21).

Regarding ***claim 11***, Klein discloses a system for authenticating information transmitted via a communications network (see Figs. 1-8), comprising a transmitting apparatus for converting an original input data into a first format (see Figs. 6 and 7, column 9, line 52-column 10, line 6), the transmitting apparatus further comprising means for computing an encrypted checksum representing the input data (steps 218-224, column 9, line 66-column 10, line 6), a receiving apparatus for receiving data in the first format from the transmitting apparatus (see Fig. 8, column 9, line 61-column 10, line 21), the receiving apparatus further comprising means for computing checksum of the received data (steps 218-222), a decrypting means for decrypting the encrypted checksum (step 220), and means for comparing the decrypted checksum with checksum of the received data, and alerting a recipient at the receiving apparatus in the event of a mismatch (see Fig. 8, steps 224-228, column 10, lines 7-21).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. **Claims 1-18** are rejected under 35 U.S.C. 103(a) as being unpatentable over Adler *et al.* (U.S. Patent Number 6,256,115) in view of Fischer (U.S. Patent Number 5,214,702).

Regarding ***claim 1***, Adler discloses a system for authenticating information communicated over a network (see abstract), comprising an originating device (see Fig. 1, node 10, column 4, line 57-column 6, line 42), the originating device comprising means for generating data representative of data received by the originating device (column 6, line 17-column 7, line 15), means for computing a checksum of the input data (column 18, lines 14-59), means for encrypting the computed checksum, thereby generating an encrypted checksum data (see abstract, column 5, line 66-column 6, line 16, and column 18, lines 14-59), means for convolving the representative data and the encrypted checksum data thereby producing a convolved data (column 18, line 42-column 19, line 24), means for communicating the convolved data to a destination device (node 14, column 4, line 62-column 6, line 42), the destination device comprising means for computing checksum of data received at the destination device, means for decrypting the encrypted checksum data from convolved data (see abstract, column 21, lines 10-30, and column 22, lines 26-42), means for comparing the decrypted checksum data with checksum computed by the destination device in order to verify the authenticity of information received by the destination device, and means for alerting a recipient at the destination device in the event of a mismatch between the decrypted checksum data and the checksum computed by the destination device.

However, Adler fails to expressly disclose if the destination device further comprises means for computing checksum of data received at the destination device, means for comparing the decrypted checksum data with checksum computed by the destination device in order to verify the authenticity of information received by the destination device, and means for alerting a recipient at the destination device in the event of a mismatch between the decrypted checksum data and the checksum computed by the destination device.

Fischer discloses a system for authenticating information communicated over a network (see abstract and Fig. 1), comprising an originating device (terminal A, column 9, lines 28-66), the originating device comprising means for generating data representative of data received by the originating device (column 9, lines 28-66, column 15, line 47-column 16, line 21), means for computing a checksum of the input data (column 15, line 47-column 16, line 21), means for encrypting the computed checksum, thereby generating an encrypted checksum data (column 9, lines 28-66, column 15, line 47-column 16, line 21), means for convolving the representative data and the encrypted checksum data thereby producing a convolved data (column 9, lines 28-66, column 15, line 47-column 16, line 21), means for communicating the convolved data to a destination device (terminals B-N, column 9, lines 28-66), the destination device comprising means for computing checksum of data received at the destination device (column 16, lines 13-43), means for decrypting the encrypted checksum data from convolved data (column 10, lines 25-65, and column 16, lines 3-27), means for comparing the decrypted checksum data with checksum computed by the destination device in order to verify the authenticity of information received by the destination device (column 16, lines 13-51), and means for alerting a recipient at the destination device in the event of a mismatch between the decrypted checksum data and the checksum computed by the destination device (column 16, lines 28-51).

Adler & Fischer are combinable because they are from the same field of endeavor, being systems that transmit encrypted data to a destination, where it is decrypted.

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to combine the teachings of Fischer with the system of Adler.

The suggestion/motivation for doing so would have been that Adler's system would have better security with the inclusion of Fischer's teachings, as the destination device can decipher the transmitted message and verify the integrity of the message, thus reducing the chance of corruption, as recognized by Fischer in column 7, lines 26-55.

Therefore, it would have been obvious to combine the teachings of Fischer with the system of Adler to obtain the invention as specified in claim 1.

Regarding ***claim 2***, Adler and Fischer disclose the system discussed above in claim 1, and Adler further teaches that the originating device comprises means for rasterizing input documents (column 2, lines 4-39, and column 5, line 66-column 6, line 42).

Regarding ***claim 3***, Adler and Fischer disclose the system discussed above in claim 1, and Adler further teaches that the originating device is a digital facsimile apparatus (column 4, line 47-column 5, line 65).

Regarding ***claim 4***, Adler and Fischer disclose the system discussed above in claim 1, and Adler further teaches that the originating device is a computer system capable of converting a digital document to a facsimile compatible format (column 5, line 66-column 6, line 42).

Regarding ***claim 5***, Adler and Fischer disclose the system discussed above in claim 4, and Adler further teaches that the computer system comprises communication means with communication software installed in the computer system (column 14, lines 5-28, and column17, line 15-column 18, line 41).

Regarding ***claim 6***, Adler and Fischer disclose the system discussed above in claim 1, and Adler further teaches that the destination device comprises a computer system comprising communication means with communication software installed in the computer system (column 9, line 46-column 10, line 45).

Regarding ***claim*** 7, Adler and Fischer disclose the system discussed above in claim 1, and Adler further teaches that information from the originating device to the destination device is communicated over a PSTN (column 5, line 12-column 6, line 64).

Regarding ***claim 8***, Adler and Fischer disclose the system discussed above in claim 1, and Adler further teaches of means for converting the convolved data into a format compatible for e-mail transmission (column 18, lines 14-59).

Regarding ***claim 9***, Adler and Fischer disclose the system discussed above in claim 1, and Adler further teaches that information from the originating device to the destination device is communicated via a wireless network (column 4, line 66-column 5, line 65, wherein the "primary network of 24 could be realized with existing data and voice networks…", thus including a wireless network).

Regarding ***claim 10***, Adler and Fischer disclose the system discussed above in claim 1, and Adler further teaches that information from the originating device to the destination device is communicated via internet (column 5, lines 12-21, and column 18, lines 14-59).

Regarding ***claim 11***, Adler discloses a system for authenticating information transmitted via a communications network (see abstract), comprising a transmitting apparatus for converting an original input data into a first format (see Fig. 1, node 10, column 4, line 57-column 6, line 42), the transmitting apparatus further comprising means for computing an encrypted checksum representing the input data (see abstract, column 5, line 66-column 6, line 16, and column 18, lines 14-59), a receiving apparatus for receiving data in the first format from the transmitting apparatus (node 14, column 4, line 62-column 6, line 42), the receiving apparatus further comprising a decrypting means for decrypting the encrypted checksum (see abstract, column 21, lines 10-30, and column 22, lines 26-42).

However, Adler fails to expressly disclose if the receiving apparatus further comprises means for computing checksum of the received data, and means for comparing the decrypted checksum with checksum of the received data, and alerting a recipient at the receiving apparatus in the event of a mismatch.

Fischer discloses a system for authenticating information transmitted via a communications network (see abstract and Fig. 1), comprising a transmitting apparatus for converting an original input data into a first format (terminal A, column 9, lines 28-66), the transmitting apparatus further comprising means for computing an encrypted checksum representing the input data (column 15, line 47-column 16, line 21), a receiving apparatus for receiving data in the first format from the transmitting apparatus (terminals B-N, column 9, lines 28-66), the receiving apparatus further comprising means for computing checksum of the received data (hashing algorithm 34, column 6, lines 13-43), a decrypting means for decrypting the encrypted checksum (column 16, lines 3-27), and means for comparing the decrypted checksum with checksum of the received data, and alerting a recipient at the receiving apparatus in the event of a mismatch (column 16, lines 28-43).

Adler & Fischer are combinable because they are from the same field of endeavor, being systems that transmit encrypted data to a destination, where it is decrypted.

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to combine the teachings of Fischer with the system of Adler.

The suggestion/motivation for doing so would have been that Adler's system would have better security with the inclusion of Fischer's teachings, as the destination device can decipher the transmitted message and verify the integrity of the message, thus reducing the chance of corruption, as recognized by Fischer in column 7, lines 26-55.

Therefore, it would have been obvious to combine the teachings of Fischer with the system of Adler to obtain the invention as specified in claim 11.

Regarding ***claim 12***, Adler and Fischer disclose the system discussed above in claim 11, and Adler further teaches that the transmitting apparatus is a digital facsimile system (column 4, line 47-column 5, line 65) (column 4, line 47-column 5, line 65).

Regarding ***claim 13***, Adler and Fischer disclose the system discussed above in claim 11, and Adler further teaches that the receiving apparatus is a digital facsimile system (column 4, line 47-column 5, line 65).

Regarding ***claim 14***, Adler and Fischer disclose the system discussed above in claim 11, and Adler further teaches that the transmitting apparatus comprises a computer system comprising a communication means with communication software installed in the computer system (column 9, line 46-column 10, line 45).

Regarding ***claim 15***, Adler and Fischer disclose the system discussed above in claim 14, and Adler further teaches of a server system in communication with the computer system (column 4, line 62-column 5, line 65).

Regarding ***claim 16***, Adler and Fischer disclose the system discussed above in claim 11, and Adler further teaches that the receiving apparatus comprises a computer system comprising a communication means with communication software installed in the computer system (column 9, line 46-column 10, line 45).

Regarding ***claim 17***, Adler and Fischer disclose the system discussed above in claim 16, and Adler further teaches that the server system is in communication with the computer system, the server system configured to receive and store the decrypted checksum along with the received data in the first format (see abstract, column 21, lines 10-30, and column 22, lines 26-42).

Regarding ***claim 18***, Adler and Fischer discloses the system discussed above in claim 17, and Fischer further teaches of an e-mail system configured to access the server system, the e-mail system being operable to receive and display the decrypted checksum along with the received data in the first format, the received data being viewed using a software capable of displaying the received data (see abstract, column 25, lines 8-54, and column 27, line 33-column 28, line 60).

As discussed above, Adler & Fischer are combinable because they are from the same field of endeavor, being systems that transmit encrypted data to a destination, where it is decrypted.

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to combine the teachings of Fischer with the system of Adler.

The suggestion/motivation for doing so would have been that Adler's system would have better security with the inclusion of Fischer's teachings, as the destination device can decipher the transmitted message and verify the integrity of the message, thus reducing the chance of corruption, as recognized by Fischer in column 7, lines 26-55.

Therefore, it would have been obvious to combine the teachings of Fischer with the system of Adler to obtain the invention as specified in claim 18.

Citation of Pertinent Prior Art

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

Brandenburg (U.S. Patent Number 5,894,516) discloses a broadcast software distribution system that employs the encryption of checksums.

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Joe Pokrzywa whose telephone number is (703) 305-0146. The examiner can normally be reached on Monday-Friday, 7:30-4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edward L. Coles can be reached on (703) 305-4712. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Joseph R. Pokrzywa
Examiner
Art Unit 2622

jrp